UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/591,708 | 06/09/2000 | Stuart J. Jacobs | 00-8010 | 2685 |

32127 7590 03/22/2007

VERIZON
PATENT MANAGEMENT GROUP
1515 N. COURTHOUSE ROAD, SUITE 500
ARLINGTON, VA 22201-2909

| EXAMINER | |
|---|---|
| HA, LEYNNA A | |
| **ART UNIT** | **PAPER NUMBER** |
| 2135 | |

| SHORTENED STATUTORY PERIOD OF RESPONSE | NOTIFICATION DATE | DELIVERY MODE |
|---|---|---|
| 3 MONTHS | 03/22/2007 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 03/22/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patents@VERIZON.COM

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/591,708 | JACOBS ET AL. | |
| | Examiner | Art Unit | |
| | LEYNNA T. HA | 2135 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *26 December 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-6 and 8-22* is/are pending in the application.

4a) Of the above claim(s) *7 and 23* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6 and 8-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. Claims 1-6 and 8-22 remains pending. Claims 7 and 23 are cancelled.

2. Claims 9-13 was previously rejected under 35 U.S.C. 101, is now withdrawn.

3. This is a Final rejection.

### *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

**4. Claims 1-6 and 8-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sudia, et al. (US 5,825,880), and further in view of Boebert, et al. (US 5,596,718).**

**As per claim 1:**

Sudia teaches in a node operative within a network of a plurality of nodes, a method for performing cryptographic-related functions comprising:

executing an application program at the node which is not secured; **(col.8, lines 21-23)**

receiving an input requiring cryptographic-related processing; **(col.8, lines 27-29)**

generating a message via the application program based on the input **(col.8, lines 45-52)**, the message representing one of a predefined set of messages **(col.8, lines 10-14 and col.11, lines 6-15)** for processing by a cryptographic processing component located within the network node; **(col.8, lines 23-27 and col.8, line 63 - col.9, line 18)**

transmitting the message to the cryptographic processing component; and **(col.8, lines 47-55 and col.10, lines 8-14)**

performing the cryptographic-related processing by the cryptographic processing component. **(col.9, lines 40-55 and col.10, lines 31-38)**

Sudia discloses human operators work in relatively unsecured areas at desktop computer or terminals where there includes a card reader which obviously is where a smart card is to be inserted (col.8, lines 20-24). Each smart card is a cryptographic processing component within an unsecured desktop (node) (col.8, lines 25-30) that is used to send messages to trusted devices which appends a digital signature using the device private signature key (col.8, lines 45-56). Hence, a smart card (a cryptographic processing component) is used to send to messages (col.8, line 63 - col.9, line 18). Sudia also discusses the smartcard may also be a signing device (col.9, lines 22-23). Although, Sudia describes plurality of unsecured desktop computers or terminals, the process of executing and performing cryptographic functions are obviously individual per node basis because Sudia mentions "a work station" (col.8, line 20). Thus, each

smart card within a desktop or node reads on the claimed "the node", that can execute application programs where the smartcard (cryptographic processing component) contains private decryption key and private signature key used to perform cryptographic related processing (col.9, lines 40-56 and col.10, lines 31-39). This reads on the claimed the node is not secured and processing by a cryptographic processing component located within the node. However, a secondary prior art is brought forth to further clarify Sudia that it would have been obvious to execute an application program at the node that is not secured and generating a message for processing by a cryptographic processing component within a node.

Boebert teaches there is a need for a mechanism for extending the trusted path form the trusted subsystem of the host computer to the user of an untrusted computer or workstation such that provide access to the workstation for normal working station activities while shielding confidential data so that it cannot be read by software executing on the unsecured workstation (col.3, lines 14-19). The computer or workstation as recited in Boebert is the claimed node. Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention was made to combine the teachings Sudia with the teaching of executing an application program at the node that is not secure of Boebert because the method ensures secure file transfers between a user of an unsecured workstation and a trusted computer while shielding confidential data so that it cannot be read by software executing on the unsecured workstation (col.3, lines 21-42).

**As per claim 2:** Sudia discloses verifying a digital signature wherein includes encrypting and decrypting data (col.6, lines 32-42), retrieving the digital certificate (col.10, lines 15-38), verifying the hierarchy (col.1, lines 24-38), and self-signed certificate processing (col.7, lines 45-52) within the node. Further, Sudia discloses certificate age checking in the form of time stamping (col.9, lines 13-16).

**As per claim 3:** See col.11, lines 9-22 and col.16, lines 35-67 discusses generating a function call message representing a request for performing a predetermined cryptographic related functions.

**As per claim 4:** Sudia discloses generating an output message via the application program wherein the output message requiring cryptographic-related processing (col.11, lines 6-10), transmitting one of predefined the messages (col.11, lines 10-13) to the cryptographic processing component (col.9, lines 9-13) to perform the cryptographic-related processing (col.9, lines 55-56), and outputting the processed message (col.11, lines 17-18).

**As per claim 5:**

Sudia teaches a computer readable medium having stored thereon a plurality of sequences of instructions that may be invoked by a plurality of predefined messages executed by a processor in an environment, which is not secure **(col.8, lines 21-29)**, cause said processor to perform a method comprising:

receiving an input representing one of predefined messages; **(col.8, lines 10-14)**

transmitting, based on the input, generating a function call message **(col.8, lines 45-55 and col.10, lines 7-13)** representing a request **(col.11, lines 6-9)** for performing a predetermined cryptographic related functions **(col.11, lines 9-22 and col.16, lines 35-67)**; and

perform the cryptographic-related processing **(col.10, lines 15-30).**

Sudia discloses human operators work in relatively unsecured areas at desk-top computer or terminals where there includes a card reader which obviously is where a smart card is to be inserted (col.8, lines 20-24). Each smart card is a cryptographic processing component within an unsecured desktop (node) (col.8, lines 25-30) that is used to send messages to trusted devices which appends a digital signature using the device private signature key (col.8, lines 45-56). Hence, a smart card (a cryptographic processing component) is used to send to messages (col.8, line 63 - col.9, line 18). Sudia also discusses the smartcard may also be a signing device (col.9, lines 22-23). Although, Sudia describes plurality of unsecured desk-top computers or terminals, the process of executing and performing cryptographic functions are obviously individual per node basis because Sudia mentions "a work station" (col.8, line 20). Thus, each smart card within a desktop or node reads on the claimed "the node", that can execute application programs where the smartcard (cryptographic processing component) contains private decryption key and private signature key used to perform cryptographic related processing (col.9, lines 40-56 and col.10, lines 31-39). This reads on the claimed the node is not secured and processing by a cryptographic processing component located within the node. However, a

secondary prior art is brought forth to further clarify Sudia that it would have been obvious to execute an application program at the node that is not secured and generating a message for processing by a cryptographic processing component within a node.

Boebert teaches there is a need for a mechanism for extending the trusted path form the trusted subsystem of the host computer to the user of an untrusted computer or workstation such that provide access to the workstation for normal working station activities while shielding confidential data so that it cannot be read by software executing on the unsecured workstation (col.3, lines 14-19). The computer or workstation as recited in Boebert is the claimed node. Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention was made to combine the teachings Sudia with the teaching of executing an application program at the node that is not secure of Boebert because the method ensures secure file transfers between a user of an unsecured workstation and a trusted computer while shielding confidential data so that it cannot be read by software executing on the unsecured workstation (col.3, lines 21-42).

**As per claim 6:** Sudia discloses verifying a digital signature wherein includes encrypting and decrypting data (col.6, lines 32-42), retrieving the digital certificate (col.10, lines 15-38), verifying the hierarchy (col.1, lines 24-38), and self-signed certificate processing (col.7, lines 45-52) within the node. Further, Sudia discloses certificate age checking in the form of time stamping (col.9, lines 13-16).

**As per claim 7: Cancelled**

**As per claim 8: See Sudia col.11, lines 6-13;** discussing the input represents a digitally signed network control message requiring verification.

**As per claim 9:**

Sudia discloses in an environment which is not secure, a cryptographic module, comprising:

a memory configured to operate within an environment which is not secure and to store a plurality of cryptographic processing programs **(col.8, lines 21-29 and col.9, lines 1-10)**, each program being invoked via one of a plurality of predefined messages; and **(col.8, lines 10-14 and col.11, lines 6-15)**

a processor configured to operate within an environment and to: **(col.8, lines 65-67)**

receive an input requiring cryptographic-related processing, **(col.8, lines 45-52)**

generates one of predefined messages based on the input, **(col.8, lines 23-27 and col.8, line 63 - col.9, line 18)**

transmit the message to the first one of the cryptographic processing programs, and **(col.8, lines 47-55 and col.10, lines 8-14)**

to perform the cryptographic-related processing. **(col.9, lines 40-55 and col.10, lines 31-38)**

Sudia discloses human operators work in relatively unsecured areas at desk-top computer or terminals where there includes a card reader which obviously is where a smart card is to be inserted (col.8, lines 20-24). Each smart

card is a cryptographic processing component within an unsecured desktop (node) (col.8, lines 25-30) that is used to send messages to trusted devices which appends a digital signature using the device private signature key (col.8, lines 45-56). Hence, a smart card (a cryptographic processing component) is used to send to messages (col.8, line 63 - col.9, line 18). Sudia also discusses the smartcard may also be a signing device (col.9, lines 22-23). Although, Sudia describes plurality of unsecured desk-top computers or terminals, the process of executing and performing cryptographic functions are obviously individual per node basis because Sudia mentions "a work station" (col.8, line 20). Thus, each smart card within a desktop or node reads on the claimed "the node", that can execute application programs where the smartcard (cryptographic processing component) contains private decryption key and private signature key used to perform cryptographic related processing (col.9, lines 40-56 and col.10, lines 31-39). This reads on the claimed the node is not secured and processing by a cryptographic processing component located within the node. However, a secondary prior art is brought forth to further clarify Sudia that it would have been obvious to execute an application program at the node that is not secured and generating a message for processing by a cryptographic processing component within a node.

Boebert teaches there is a need for a mechanism for extending the trusted path form the trusted subsystem of the host computer to the user of an untrusted computer or workstation such that provide access to the workstation for normal working station activities while shielding confidential data so that it cannot be

read by software executing on the unsecured workstation (col.3, lines 14-19). The computer or workstation as recited in Boebert is the claimed node. Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention was made to combine the teachings Sudia with the teaching of executing an application program at the node that is not secure of Boebert because the method ensures secure file transfers between a user of an unsecured workstation and a trusted computer while shielding confidential data so that it cannot be read by software executing on the unsecured workstation (col.3, lines 21-42).

**As per claim 10:** Sudia discloses verifying a digital signature wherein includes encrypting and decrypting data (col.6, lines 32-42), retrieving the digital certificate (col.10, lines 15-38), verifying the hierarchy (col.1, lines 24-38), and self-signed certificate processing (col.7, lines 45-52) within the node. Further, Sudia discloses certificate age checking in the form of time stamping (col.9, lines 13-16).

**As per claim 11:** **See Sudia col.7, lines 34-45;** discussing transmit a function call to the first cryptographic processing program.

**As per claim 12:** **See Sudia col.11, lines 6-13;** discussing transmit the result of the cryptographic-related processing to an application program.

**As per claim 13:**

Sudia discusses in an environment which is not secure, a cryptographic module, comprising:

means, operative in the environment which is not secure **(col.8, lines 21-24)**, for storing a plurality of cryptographic processing programs that is invoked via one of the plurality of predefined messages; **(col.8, lines 10-11 and col.10, lines 10-14)**

means, operative in the environment, for receiving an input requiring cryptographic-related processing; **(col.8, lines 23-27 and col.8, line 63 - col.9, line 18)**

means, operative in the environment, for generating the one of predefined messages based on the input; **(col.8, lines 45-55)**

means, operative in the environment, for transmitting the message to the first one of the cryptographic processing programs, and **(col.8, lines 47-55 and col.10, lines 8-14)**

means, operative in the environment, for performing the cryptographic-related processing. **(col.9, lines 40-55 and col.10, lines 31-38)**

Sudia discloses human operators work in relatively unsecured areas at desk-top computer or terminals where there includes a card reader which obviously is where a smart card is to be inserted (col.8, lines 20-24). Each smart card is a cryptographic processing component within an unsecured desktop (node) (col.8, lines 25-30) that is used to send messages to trusted devices which appends a digital signature using the device private signature key (col.8,

lines 45-56). Hence, a smart card (a cryptographic processing component) is used to send to messages (col.8, line 63 - col.9, line 18). Sudia also discusses the smartcard may also be a signing device (col.9, lines 22-23). Although, Sudia describes plurality of unsecured desk-top computers or terminals, the process of executing and performing cryptographic functions are obviously individual per node basis because Sudia mentions "a work station" (col.8, line 20). Thus, each smart card within a desktop or node reads on the claimed "the node", that can execute application programs where the smartcard (cryptographic processing component) contains private decryption key and private signature key used to perform cryptographic related processing (col.9, lines 40-56 and col.10, lines 31-39). This reads on the claimed the node is not secured and processing by a cryptographic processing component located within the node. However, a secondary prior art is brought forth to further clarify Sudia that it would have been obvious to execute an application program at the node that is not secured and generating a message for processing by a cryptographic processing component within a node.

Boebert teaches there is a need for a mechanism for extending the trusted path form the trusted subsystem of the host computer to the user of an untrusted computer or workstation such that provide access to the workstation for normal working station activities while shielding confidential data so that it cannot be read by software executing on the unsecured workstation (col.3, lines 14-19). The computer or workstation as recited in Boebert is the claimed node. Therefore, it would have been obvious for a person of ordinary skills in the art at

the time of the invention was made to combine the teachings Sudia with the teaching of executing an application program at the node that is not secure of Boebert because the method ensures secure file transfers between a user of an unsecured workstation and a trusted computer while shielding confidential data so that it cannot be read by software executing on the unsecured workstation (col.3, lines 21-42).

**As per claim 14:**

Sudia discusses a method of performing cryptographic-related functions in a node coupled to other nodes in a network environment which is not secure, the node includes an application program for handling communications with the other nodes the method comprising:

receiving in said node within the environment which is not secure **(col.8, lines 21-24)** an input requiring cryptographic-related processing; **(col.7, lines 34-40 and lines 53-54)**

generating in said node within the environment a predefined message **(col.8, lines 10-14 and col.11, lines 6-15)** based on the input, the message one of a plurality of predefined message usable by of the cryptographic processing programs executed by the network node; **(col.8, lines 23-27 and col.8, line 63 - col.9, line 18)**

transmitting in said node within the environment a predefined message to the cryptographic processing program; **(col.8, lines 47-55 and col.10, lines 8-14)**

performing in said node within the environment, via cryptographic processing program the desired cryptographic-related operation. **(col.9, lines 40-55 and col.10, lines 31-38)**

Sudia discloses human operators work in relatively unsecured areas at desk-top computer or terminals where there includes a card reader which obviously is where a smart card is to be inserted (col.8, lines 20-24). Each smart card is a cryptographic processing component within an unsecured desktop (node) (col.8, lines 25-30) that is used to send messages to trusted devices which appends a digital signature using the device private signature key (col.8, lines 45-56). Hence, a smart card (a cryptographic processing component) is used to send to messages (col.8, line 63 - col.9, line 18). Sudia also discusses the smartcard may also be a signing device (col.9, lines 22-23). Although, Sudia describes plurality of unsecured desk-top computers or terminals, the process of executing and performing cryptographic functions are obviously individual per node basis because Sudia mentions "a work station" (col.8, line 20). Thus, each smart card within a desktop or node reads on the claimed "the node", that can execute application programs where the smartcard (cryptographic processing component) contains private decryption key and private signature key used to perform cryptographic related processing (col.9, lines 40-56 and col.10, lines 31-39). This reads on the claimed the node is not secured and processing by a cryptographic processing component located within the node. However, a secondary prior art is brought forth to further clarify Sudia that it would have been obvious to execute an application program at the node that is not secured and

generating a message for processing by a cryptographic processing component within a node.

Boebert teaches there is a need for a mechanism for extending the trusted path form the trusted subsystem of the host computer to the user of an untrusted computer or workstation such that provide access to the workstation for normal working station activities while shielding confidential data so that it cannot be read by software executing on the unsecured workstation (col.3, lines 14-19). The computer or workstation as recited in Boebert is the claimed node. Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention was made to combine the teachings Sudia with the teaching of executing an application program at the node that is not secure of Boebert because the method ensures secure file transfers between a user of an unsecured workstation and a trusted computer while shielding confidential data so that it cannot be read by software executing on the unsecured workstation (col.3, lines 21-42).

**As per claim 15:** **See Sudia on col.11, lines 38-52;** discussing returning the result of the performing to the application program.

**As per claim 16:** Sudia discusses the method of requests for digital generation, verification, data encryption and decryption (col.6, lines 32-42), retrieval of digital certificate (col.10, lines 15-38), verifying the hierarchy (col.1, lines 24-38), self-signed certificate processing (col.7, lines 45-52), and certificate age checking in the form of time stamping (col.9, lines 13-16).

**As per claim 17: See Sudia col.6, lines 4-19 and col. 7, lines 8-15;** discussing the RSA signature scheme and the MD5 scheme.

**As per claim 18: See Sudia col.6, lines 4-19 and col. 7, lines 8-15;** discussing the RSA signature scheme and the MD5 scheme.

**As per claim 19: See Sudia col.6, lines 4-19 and col. 7, lines 8-15;** discussing the RSA signature scheme and the MD5 scheme.

**As per claim 20: See Sudia col.6, lines 4-19 and col. 7, lines 8-15;** discussing the RSA signature scheme and the MD5 scheme.

**As per claim 21: See Sudia col.6, lines 24-30;** discusses accessing a remote server via the network to retrieve cryptographic related information.

**As per claim 22:**

Sudia discloses a computer-readable medium that stores instructions executable by at least one processor in an environment which is not secure to perform a method for providing cryptographic-related functions, the method comprising:

receiving in at least one processor in the environment which is not secure a first function call from a predefined list a first function call from a predefined list of function calls **(col.8, lines 10-14 and col.11, lines 6-15)** representing available cryptographic-related functions executable by the at least one processor; **(col.8, lines 23-27 and col.8, line 63 - col.9, line 18)**

generating in at least one processor in the environment a request message based on the first function call, a for cryptographic processing to further transmit the request message representing a request for processing by **(col.8,**

**lines 45-52)** a cryptographic processing module executed by the at least one processor; **(col.8, line 63 - col.9, line 10)**

transmitting in at least one processor in the environment the request message to the cryptographic processing module; and **(col.8, lines 47-55 and col.10, lines 8-14)**

performing in at least one processor in the environment the cryptographic-related processing. **(col.9, lines 40-55 and col.10, lines 31-38)**

Sudia discloses human operators work in relatively unsecured areas at desk-top computer or terminals where there includes a card reader which obviously is where a smart card is to be inserted (col.8, lines 20-24). Each smart card is a cryptographic processing component within an unsecured desktop (node) (col.8, lines 25-30) that is used to send messages to trusted devices which appends a digital signature using the device private signature key (col.8, lines 45-56). Hence, a smart card (a cryptographic processing component) is used to send to messages (col.8, line 63 - col.9, line 18). Sudia also discusses the smartcard may also be a signing device (col.9, lines 22-23). Although, Sudia describes plurality of unsecured desk-top computers or terminals, the process of executing and performing cryptographic functions are obviously individual per node basis because Sudia mentions "a work station" (col.8, line 20). Thus, each smart card within a desktop or node reads on the claimed "the node", that can execute application programs where the smartcard (cryptographic processing component) contains private decryption key and private signature key used to perform cryptographic related processing (col.9, lines 40-56 and col.10, lines 31-

39). This reads on the claimed the node is not secured and processing by a cryptographic processing component located within the node. However, a secondary prior art is brought forth to further clarify Sudia that it would have been obvious to execute an application program at the node that is not secured and generating a message for processing by a cryptographic processing component within a node.

Boebert teaches there is a need for a mechanism for extending the trusted path form the trusted subsystem of the host computer to the user of an untrusted computer or workstation such that provide access to the workstation for normal working station activities while shielding confidential data so that it cannot be read by software executing on the unsecured workstation (col.3, lines 14-19). The computer or workstation as recited in Boebert is the claimed node. Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention was made to combine the teachings Sudia with the teaching of executing an application program at the node that is not secure of Boebert because the method ensures secure file transfers between a user of an unsecured workstation and a trusted computer while shielding confidential data so that it cannot be read by software executing on the unsecured workstation (col.3, lines 21-42).

***Response to Arguments***

**5. Applicant's arguments filed 12/26/2006 have been fully considered but they are not persuasive.**

Applicant's arguments with respect to claims 1-6 and 8-22 remains rejected in view of the Sudia and Boebert combination.

Regarding applicant's argument throughout pages 12-14 that the prior art does not teach a node that is not secure to conduct cryptographic activity in or at the one node. Sudia discloses human operators work in relatively unsecured areas at desk-top computer or terminals where there includes a card reader which obviously is where a smart card is to be inserted (col.8, lines 20-24). Thus, each smart card for use with each workstation or desktop reads on the claimed "the node". Each smart card is a cryptographic processing component within an unsecured desktop (node) (col.8, lines 25-30). Although, Sudia describes plurality of unsecured desk-top computers or terminals, the process of executing and performing cryptographic functions are obviously individual per node basis because Sudia mentions "a work station" (col.8, line 20). This reads on the claimed the node is not secured and processing by a cryptographic processing component located within the node. Therefore, the smartcard or signing device is not being referred as a node or vault or message server.

However, a secondary prior art is brought forth to further clarify Sudia that it would have been obvious to execute an application program at the node that is not secured and generating a message for processing by a cryptographic processing component within a node. Boebert teaches there is a need for a

mechanism for extending the trusted path form the trusted subsystem of the host computer to the user of an untrusted computer or workstation such that provide access to the workstation for normal working station activities while shielding confidential data so that it cannot be read by software executing on the unsecured workstation (col.3, lines 14-19). Thus, it would have been obvious to combine Sudia and Boebert because executing an application program at the node that is not physically secure can still be extended to ensure secure file transfers between an unsecured workstation and a for the trusted computer (col.3, lines 21-42).

Examiner traverses the argument on Page 15, that the title and abstract of Boebert recites secure communication over a secure computer network. As such, Boebert's invention is for secure communication just like applicant's claimed invention. However, secure communication over a secure network does not read or mean that the request or initial execution of an application is from a secure node either. Boebert teaches a method and apparatus for ensuring secure communications over an unsecured communications medium between a user working on an unsecured workstation or computer and a host computer where the data transferred is intercepted, encrypted and transmitted in packets to the host computer (col.3, lines 23-30). The claimed broadly recites the executing and performing or processing cryptographic related functions at or in the (one) node and that the preamble merely disclosing a node operative within a network of a plurality of nodes. The claimed invention is focusing communication

on or within the node. Thus, the claim does not suggest any communication being received or transmitted over or through a network.

Boebert reads on the claimed executing an application program at the node that is not secured and cryptographic related processing within the node. Therefore, examiner traverses the argument on page 16 because Sudia in combination with Boebert teaches the claimed invention.

Examiner traverses the argument brought forth on page 16-19, regarding a previous prior art (Veil) used in two previous office actions ago (5/4/2006). Examiner will not respond to these arguments during this office action because Veil was not even applied on during the last office action (10/19/2006) to teach the claimed invention.

***Conclusion***

**6. THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the

mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

LHa